



# Auditoría, Evaluación, TEST DE SEGURIDAD

LA PROPUESTA FINAL, ES EL EJEMPLO QUE PROPONE LA METODOLOGÍA ABIERTA DENOMINADA OSSTMM (OPEN-SOURCE SECURITY METHODOLOGY MANUAL)



**Alejandro Corletti Estrada**

DIRECTOR DIVISIÓN  
SEGURIDAD  
NCS

La problemática actual de seguridad en la masa de las empresas tiene un trasfondo oculto que debe ser encarado por sus responsables, si se tuviera que resumir en pocas líneas se podría presentar como sigue:

- Creciente nivel de vulnerabilidades y mayor grado de exposición de recursos.
- Imposibilidad de contar con personal especializado y actualizado.
- Dificultad para cuantificar su nivel de riesgo.

Al solicitar apoyo de consultoría a empresas especializadas, es casi una norma general que le indiquen que el primer paso a seguir es la realización de una «auditoría de seguridad»

A lo largo de este texto se tratará de establecer una relación entre:

- Lo que el cliente verdaderamente necesita.

- Cómo se puede clasificar lo que habitualmente se engloba bajo «Auditorías de seguridad».

- Si es posible respetar algún método que permita repetir esta tarea y obtener índices de evolución.

La propuesta final, es el ejemplo que propone esta metodología abierta denominada OSSTMM (Open-Source Security Methodology Manual), la cual

ción de seguridad, penetration test, OSSTMM.

## Lo que el cliente verdaderamente necesita

La hipótesis que se presenta trata de reflejar una problemática de seguridad que se encuentra en exponencial crecimiento y con una voráGINE tal que no permite a los responsables de sistemas de las «pymes», mantener personal al tanto de lo que sucede día a día. Es más, este hecho se podría considerar casi como asumido por esta línea de empresas, es decir, los gerentes de sistemas ya son plenamente conscientes que un alto nivel de capacitación en seguridad es una cuestión cara y cuya relación coste/beneficio, tiene un cierto límite marcado por el conocimiento básico de seguridad de sus administradores y un claro umbral, superado el cual (por situaciones puntuales o por periodicidad), se debe solicitar el apoyo externo.

Este apoyo externo, cada vez más frecuente (por la simple relación coste/beneficio planteada), se podría englobar en dos grandes causas:

- **Problemas puntuales de seguridad:** Cuando ocurren hechos que su-

Un trabajo de auditoría externa es la mejor oportunidad para cuantificar el nivel de seguridad

no se desea remarcar como mejor o peor que cualquier otra, sino simplemente como una guía gratuita a tomar como referencia ante la necesidad que suele tener todo responsable de sistemas al pedir este tipo de asesoramiento y/o contratarlos.

Palabras clave: Auditoría y evalua-



www.freeimages.co.uk

peran el conocimiento básico de sus administradores.

■ **Periódicos:** Cuando se ha llegado a una situación que hace necesaria una cierta evaluación de alguna plataforma, un nuevo servicio o una «Cuantificación del nivel de riesgo»

Al solicitar este apoyo de consultoría a empresas especializadas, es casi una norma general que le indiquen que el primer paso a seguir es la realización de una auditoría de seguridad. Este consejo puede considerarse válido, pues es muy difícil poder evaluar o tomar cualquier acción con escaso conocimiento de la infraestructura que se posee, pero aquí es donde hay que detenerse seriamente para plantear lo que el cliente verdaderamente necesita y cómo llevarlo a cabo.

El cliente necesita:

- Soluciones.
- Garantías.

■ Índices (o parámetros).

iii Y NADA MÁS !!!, pues partimos de la hipótesis que no es un especialista en seguridad, y para eso confía en la empresa consultora.

**El tiempo de solución dependerá de la «Expertiz» del auditor y de sus ganas de involucrarse con el cliente**

■ **Soluciones:** El cliente es consciente que tiene un problema, es muy frecuente que no tenga claro de qué se trata o de dónde proviene, pero está

seguro que lo tiene. Independientemente de todo el trabajo de análisis, detección y evaluación que se realice, el resultado final del mismo debe proporcionar descripciones muy claras de cómo solucionarlo, pues caso contrario, no tendría sentido la totalidad del trabajo. Este punto es de vital interés, pues es difícil para el experto, bajar al nivel de alguien que no tiene por qué tener idea de seguridad y explicarle con todas las letras los pasos que debe seguir para solucionar el mismo.

■ **Garantías:** Todo el trabajo que se realice debe culminar ofreciendo dos tipos de garantías:

- ◆ Que se ha detectado la masa de los problemas de seguridad: Este aspecto no es trivial, pues acorde al tipo de trabajo que se realice y al tiempo dedicado, se podrá profundizar más o menos. Lo que no se puede dudar, es que



durante el proceso de contratación, hay que hablar claro y dejar constancia de hasta dónde llegará el trabajo a realizar, pues no se puede aducir al finalizar esta actividad que determinadas actividades no se han realizado, o peor aún, dejar dudas sobre el nivel de seguridad de su infraestructura, pues esa parte no se había contratado, etc...

- ◆ Que al aplicar las soluciones recomendadas, el nivel de riesgo se reduce a los índices deseados, o mejor aún, que lo que se propone es «la mejor solución» a sus problemas, pues es lo que recomiendan los especialistas del tema.

En definitiva, con garantías se quiere expresar que luego de la actividad que se realice, el cliente puede encarar las soluciones recomendadas, confiando en que es su mejor opción y que

al aplicar las mismas, su nivel de riesgo ha mejorado sensiblemente.

*NOTA: Una excusa «Omnipresente» y bastante desagradable para evadir garantías (aunque lamentablemente*

**La problemática actual de seguridad en la masa de las empresas tiene un trasfondo oculto que debe ser encarado por sus responsables**

*no deja de ser cierta), es que surgen nuevas vulnerabilidades día a día, por lo tanto una vez finalizada toda activi-*

*dad, «No se puede garantizar la seguridad absoluta aplicando las soluciones propuestas», pues mañana habrá algo nuevo que afecte a la infraestructura..... Que pena..... (Confianza, seriedad, sinceridad..... etc, etc, etc)*

■ **Índices (o parámetros):** Desde mi enfoque personal, creo que uno de los problemas más grandes que tiene un gerente de sistemas es «Cuantificar la seguridad», pues como todos pueden apreciar es un «bien intangible». SE DEBE HACER TODO ESFUERZO POSIBLE PARA PONERLE NÚMEROS a la misma. Ya hay varias estrategias a seguir al respecto y en Internet se puede encontrar mucho de esto (ESPACIO PARA PUBLICIDAD: Recomiendo que miren un método que he propuesto hace tiempo que lo denominé «Matriz de Estado de Seguridad», está publicado en varias web. Su objetivo es aplicar todos los indicadores objetivos posi-

## Los parámetros más importantes a considerar son:

◆ **CRITICIDAD:** Este parámetro refleja el daño que puede causar a ese sistema la explotación de esa vulnerabilidad por quien no debe.

◆ **IMPACTO:** Independientemente de la criticidad de una vulnerabilidad encontrada, esta puede causar daño a sistemas que son el sustento de la empresa, que mantienen datos de alta clasificación (LOPD), o una fuerte pérdida de imagen de empresa, etc. O por el contrario, puede ser Crítica para ese servicio, pero el mismo no cobra mayor interés para el buen funcionamiento de la empresa.

◆ **VISIBILIDAD:** Este indicador puede servir como multiplicador de los anteriores, pues no posee el mismo ries-

go un servidor de Internet «Front End», que uno interno de la empresa con accesos restringidos.

◆ **POPULARIDAD:** Este parámetro, si bien puede ser muy discutido, permite indicar el grado de «visitas, conexiones o sesiones» que posee un sistema. El empleo o no de este indicador permite considerar, que si existiere una vulnerabilidad sobre el mismo, se puede suponer que tiene mayor grado de «exposición» que el resto. Se admite aquí que puede ser valorado o no.

◆ **MAGNITUD:** Cuántos sistemas afecta. Este parámetro es muy interesante tenerlo en cuenta por niveles, es decir una misma plataforma puede estar conformada por varios sistemas, pero también exis-

ten sistemas que forman parte de varias plataformas, que permiten el paso hacia ellas, que autentican, que filtran, que monitorizan, etc. Es decir, hay plataformas cuya magnitud «Directa» es muy clara y dependen únicamente de ellas, pero hay otras que para su funcionamiento necesitan la participación de otros elementos. En concreto, una cadena se corta por el eslabón más débil, por lo tanto, si no se considera la magnitud de una infraestructura, y se solucionan o evalúan únicamente los aspectos puntuales de cada host, el resultado no es el óptimo.

◆ **FACILIDAD DE EXPLOTACIÓN:** Una determinada vulnerabilidad, puede presentarse desde la ejecución de una simple herramienta pública en Internet y desde allí mismo, hasta una elaborada técnica



bles, dejando de lado la subjetividad). El no contar con índices o parámetros, ocasiona dos grandes perjuicios:

- ◆ Desconocimiento del grado de seguridad y de la evolución del mismo, no pudiendo plantear objetivos o umbrales a cumplir (¡¡muy negativo!!).
- ◆ Imposibilidad de demostrar el ROI en temas de seguridad ante la dirección de la empresa (¡¡¡Catastrófico!!!).

Un trabajo de auditoría externa es la mejor oportunidad para cuantificar el nivel de seguridad, pues todo especialista en el tema posee la "expertiz" necesaria para jugar con ellos, promediando valores.

Por último, relacionado a las métricas de seguridad, es muy interesante la lectura del modelo que propone NIST a través del documento «Security Metrics Guide for Information



www.freeimages.co.uk

Technology Systems», el mismo desarrolla una métrica de seguridad basada en el alcance de objetivos y metas, lo que se plasma en resultados, de

forma muy precisa. El mismo puede ser descargado en: <http://csrc.nist.gov/publications/nistpubs/800-55/sp800-55.pdf>. ◆

de intrusión, que conlleva amplios conocimientos y pasos por parte del ejecutante. En este valor entra también en juego el grado de visibilidad del sistema, el grado de segmentación interna, la autenticación, el control de accesos, etc.

◆ **FACILIDAD O COSTE DE SOLUCIÓN:** Este valor es muy subjetivo y debe ser evaluado con mucho cuidado pues es el punto de partida para planificar las soluciones. Se presentan aquí muchas combinaciones y a mi juicio es el parámetro que determina la «Expertiz» de una auditor, pues si realmente sabe, será capaz de interpretar con mayor claridad la problemática del cliente y proponerle un plan de acción «realista y eficiente» para los recursos del cliente. Se debe tener en cuenta aquí no solo la simple recomen-

dación, sino como cada una de ellas puede o no ser aplicada (pues habrá aplicaciones o servicios que no lo permitan), puede involucrar a muchos dispositivos más, puede ocasionar actualizaciones de hardware y software, rediseños, caídas de sistemas, etc...

◆ **TIEMPO DE SOLUCIÓN:** Es un parámetro muy relacionado con el anterior, y nuevamente dependerá de la «Expertiz» del auditor y de sus ganas de involucrarse con el cliente para tener en cuenta todos sus sistemas. Una de las mayores satisfacciones para el auditor (lo digo por experiencia propia) es poder entregarle al cliente un cronograma de cómo emprender las soluciones, con todo el nivel de detalle posible (Gant, hitos, valores a alcanzar mes a mes, recursos, priorida-

des, objetivos, etc), si se llega a esto es porque el auditor, se ha involucrado en tal medida con la empresa, que conoce hasta el último detalle a considerar para poder estimar este «Project». Esto para el cliente es lo máximo que puede desear, pues le permite organizar su plan de acción, presentarlo a la dirección de la empresa y acorde a los recursos que obtenga, definirá su estrategia al corto/medio plazo, para cumplir las acciones aceptadas. Se debe considerar también que es la mejor forma que posee la dirección de realizar el seguimiento del dinero que invirtió, pues los hitos serán todo lo claros que hagan falta. Este aspecto sin lugar a dudas, si se hacen bien las cosas, incrementará la confianza y los fondos que la gerencia informática tendrá para el próximo ejercicio.